	Georgia Technology Authority	
Title:	**Information Security Infrastructure**	
PSG Number:	SS-08-005.01	**Topical Area:** Security
Document Type:	Standard	**Pages:** 3
Issue Date:	3/31/08	**Effective Date:** 3/31/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Sets standards for creating an information security program and infrastructure.	

PURPOSE

In accordance with the Enterprise Information Security Infrastructure Policy, each Agency has the responsibility to exercise due diligence and due care in support of the State of Georgia's commitment to protecting its information assets, as well as for compliance with State and Federal regulatory requirements. This standard details the basic elements of an information security infrastructure.

SCOPE, AUTHORITY, ENFORCEMENT, EXCEPTIONS:

See Enterprise Information Security Charter (Policy)

STANDARD

Any agency that creates, uses, or maintains information assets for the State of Georgia, shall also establish, document, implement and maintain an internal information security infrastructure consisting of the following program elements:

- A Security management organization
- A risk management framework consistent with that recommended by the National Institute of Standards and Technology (NIST) (ref. http://csrc.nist.gov/sec-cert/risk-framework.html
- A Disaster Recovery and Business Continuity Plan/s
- An Incident Management and Response capability
- Security Education and Awareness component
- Internal policies and procedures necessary to meet agency specific business security needs or augment security requirements imposed on such agency by state and/or federal regulations.
- Assessment, Compliance and Enforcement mechanisms

REFERENCES

Reference the National Institute of Standards (NIST) Special Publication 800-12 Introduction to Computer Security (NIST Handbook) located at for more guidance on the information security infrastructure:
http://csrc.nist.gov/publications/nistpubs/index.html

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

Security Awareness Program (Policy)
Security Education and Awareness (Standard)
Information Security Management Organization (Standard)

TERMS and DEFINITIONS

FISMA – Federal Information Security Management Act requires each [federal] agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Risk Management is the process of measuring, or assessing risk and developing strategies to manage it. Strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk. It is the selection and specification of security controls necessary to protect individuals and the operations and assets of the organization as part of an organization-wide information security program that involves the *management of organizational risk*---that is, the risk to the organization or to individuals associated with the operation of an information system. The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system.

Disaster Recovery Plan (DRP) – is a comprehensive statement of consistent actions to be taken by an organization to respond quickly to a disaster or serious interruption of service to stabilize and restore critical functions. The plan should be documented and tested to ensure its effectiveness in continuing operations or restoration and availability of critical resources in the event of a disaster.

Business Continuity Plan (BCP) – An ongoing management and governance process that provides a framework for building resilience into an organization by creating and maintaining viable recovery strategies and plans. It is a holistic management process that ensures the necessary steps are taken to identify potential threats to the organization and its resources, the impact of potential losses, and to maintain its viability before, during, and after a catastrophic event.

Incident Management - is the systematic approach to preventing incidents in an information security infrastructure; responding to incidents when they occur and reporting incidents to the proper escalation points.

Note: The PSG number was changed from S-08-005.01 on September 1, 2008